IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Steven Branigan
Hal Joseph Burch
William R Cheswick

CASE 1-1-7

Serial No. 09/578633 **Group Art Unit** 2131

Filed May 25, 2000

Examiner Syed Zia

Title Method And Apparatus For Host Probing

MAILSTOP APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

SIR:

APPEAL BRIEF

Enclosed is an **Appeal Brief** in the above-identified application.

The Commissioner is authorized to charge the requisite appeal brief filing fee under 37 CFR 41.20(b)(2) to **Deposit Account No. 12-2325.** In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 12-2325** as required to correct the error.

Respectfully,

Donald P. Dinella, Attorney
Reg. No. 39961
908-582-8582.

Date: December 6, 2005

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030

Date of Deposit Dec 6, 2005

I hereby certify that this correspondence is being deposited with the United States Postal Service First Class Mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated above.

Catherine F. Dugan
Printed name of person mailing paper

Catherine F. Dugan
Signature of person mailing paper

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of Patent Application of: Steven Branigan et al.

Case: 1-1-7

Serial No.: 09/578,633

Filed: May 25, 2000

Examiner: Syed Zia

Group Art Unit: 2131

Title: Method and Apparatus For Host Probing

MAILSTOP APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

SIR:

APPEAL BRIEF

Applicants, your Appellants herein, hereby appeal the rejections contained in the outstanding Office Action, dated September 21, 2005, of claims 1-3, 6-12, 14-24 and 26-27 of the above-identified patent application.

I. Real Party In Interest

The real party in interest in this appeal is Lucent Technologies Inc., the assignee of the entire right, title and interest to this invention as per the Assignment and Agreement recorded, on May 25, 2000, in the United States Patent and Trademark Office at Reel/Frame 010852/0648.

II. Related Appeals and Interferences

None.

III. Status of Claims

Claims 4, 5, 13 and 25 have been previously cancelled. Claims 1-3, 6-12, 14-24 and 26-27 are pending in the above-identified patent application.

Claims 1, 10, 16, 21 and 24 stand rejected under §112, first paragraph, as failing to comply with the enablement requirement.

Claims 7, 20, 23 stand separately rejected under §112, first paragraph, as failing to comply with the enablement requirement.

Claims 1-3, 6-12 14-24 and 26-27 stand rejected under 35 USC § 102(e) as being anticipated by U.S. Patent No. 6,298,445 issued to Shostack et al. (hereinafter "Shostack").

Claim 14 stands rejected under 35 USC § 103(a) as being unpatentable over Shostack in view of U.S. Patent No. 6,212,561 issued to Sitaraman et al. (hereinafter "Sitaraman").

The rejection of all pending claims is appealed.

IV. Status of Amendments

The claims stand last amended in accordance with an Amendment/Reply made by Applicants on June 7, 2005 and filed concurrently with a Request for Continued Examination under 37 CFR § 1.114, entered by the Examiner in the outstanding Office Action, dated September 21, 2005 (hereinafter the "Office Action").

V. Summary of Claimed Subject Matter

The aspects of Applicants' invention, as set forth in the currently pending claims, are directed at ascertaining the integrity of a communications network and thereby identifying potential security risks across the perimeter of such network. An aspect of the invention is directed to the determination of a security characteristic of a host (or hosts) associated with a first communications network wherein the security characteristic is a measure of connectivity between the first communications network and a second communications network. That is, the host (associated with a first network) is probed with a particular packet, where such packet is intentionally configured with a source address which is associated with the second communications network, and the

connectivity measure is determined as function of a response from the probed host to the particularly configured packet (see, e.g., Applicants' Specification, page 4, line 27 – page 5, line 6; and page 8, lines 20-22).

Importantly, the source address is selected such that the IP address is external to the probed host's network, that is, the originator address is "false or derived" in that it does not originate from an actual host request (see, e.g., Applicants' Specification, page 9, lines 25-29). Thus, in accordance with the claimed invention, the source address (forming part of the specially configured probe packet) is selected independent of any actual request made from the second host to the first host. Thus, by probing the connectivity of the particular host(s) within a network, utilizing the probe packet configured in accordance with the claimed invention, an analysis of the network can be made to identify potential security risks across the perimeter of the particular network.

To be clear, the Applicants recognize that "spoofing", i.e., the faking of the sending address of a transmission in order to gain illegal entry into a secure system (see, e.g., a general definition available at http://www.techweb.com/encyclopedia; or Shostack at column 1, line 64 – column 2, line 3) is not new. Indeed, Applicant William Cheswick in the subject Application is a recognized Internet security expert (see, e.g., the enclosed references to Applicants' Amendment, dated April 7, 2004, in the subject application; a copy of such references being enclosed in the evidence appendix hereto) intimately familiar with spoofing and spoofed packets. Heretofore, the well-known use of spoofed packets (by unauthorized users or hackers) is directed to gaining illegal entry into a secure system.

In contrast, Applicants have realized that spoofed packets can serve different purposes (and non-malicious) by providing an enhanced security tool for discovering the connectivity between networks. This connectivity measure, in turn, can be used by system administrators to prevent malicious attacks (including but not limited to malicious spoofing). Advantageously, Applicants have realized that using the so-called "spoofed probe packet" (see, e.g., Applicants' Specification, page 9, line 15 through page 10, line 20) the connectivity of certain hosts can be measured and such connectivity measure can be used to identify potential unsecure or "rogue" connections between the probed host and some other host on the second communications network (see, e.g., Applicants'

Specification, page 10, lines 5-7; and FIG. 2). The probe packet, in accordance with this aspect of the invention, is not used for malicious purposes in gaining illegal entry into the first or second communications network—but rather—for non-malicious purposes in providing an enhanced security tool for discovering the connectivity between networks. Each of the currently pending independent claims includes claim language directed at these aspects of the invention.

Said another way, Applicants' claimed invention is directed at discovering connectivity of, or between, a host machine (or host machines) as a function of a response (or absence thereof) to a specifically configured probe packet. In brief, it is at least the determination of such connectivity measure using the probe packet configured in accordance with the invention, and therefore the discovery of applying spoofed packets for non-malicious purposes, that are the contributions advanced by the Applicants over the cited prior art.

VI. Grounds of Rejection To Be Reviewed on Appeal

The grounds of rejection to be reviewed on this Appeal are:

Claims 1, 10, 16, 21 and 24 stand rejected under §112, first paragraph, as failing to comply with the enablement requirement.

Claims 7, 20, 23 stand separately rejected under §112, first paragraph, as failing to comply with the enablement requirement.

Claims 1-3, 6-12 14-24 and 26-27 stand rejected under 35 USC § 102(e) as being anticipated by Shostack.

Claim 14 stands rejected under 35 USC § 103(a) as being unpatentable over Shostack in view of Sitaraman.

VII. Argument

1. Rejection of Claims 1, 10, 16, 21 and 24 under 35 USC § 112, first paragraph

The Office Action rejected claims 1, 10, 16, 21 and 24 under 35 USC § 112, first paragraph, as failing to comply with the enablement requirement, in particular, with respect to the claimed "security characteristic" and "an indication of connectivity"

subject matter. In so rejecting such claims, the Examiner asserts (see, Office Action, page 6) that "the claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention."

With respect to the claimed "security characteristic" subject matter, such subject matter is supported and described in at least the following passages in Applicants' Specification: (i) page 4, lines 22-30; (ii) page 8, lines 1-11; (iii) page 10, line 5-28; (iv) page 6, lines 10-26; and (v) page 5, lines 1-6. At a minimum, such passages from Applicants' Specification enable one skilled in the art to recognize that the claimed "security characteristic" of Applicants' invention is directed to identifying potential security risks across the perimeter of a network (see, e.g., Applicants' Specification, page 4, lines 27-30; and page 8, lines 17-22) which, in turn, is the "determining a security characteristic of the probed host" as claimed by Applicants. Examples of such security risks will be appreciated by those skilled in the art, and Applicants set forth a number of such exemplary security risks in their Specification at page 2, line 28 through page 3, line 10; and page 1, line 28 through page 2, line 10. That is, the security characteristic of the probed host, in accordance with the invention, is whether such probed host poses a security risk across the perimeter of the associated network. This feature of the invention is supported by the above-referenced passages of Applicants' Specification in enabling one skilled in the art to make and/or use the claimed security aspects of Applicants' claimed invention.

With respect to the claimed "an indication of connectivity", such subject matter is supported and described in at least the following passages of Applicants' Specification: (i) page 5, lines 1-6; (ii) page 5, lines 26-29; (iii) page 8, lines 1-22; (iv) page 9, line 15 through page 11, line 14; and (v) FIG. 2. At a minimum, such passages from Applicants' Specification enable one skilled in the art to recognize that the claimed "indication of connectivity" of Applicants' invention is directed at discovering connectivity of, or between, a host machine (or host machines) as a function of a response (or absence thereof) to the specifically configured probe packet. As will be recognized by one skilled in the art the "connectivity" aspect of the claimed invention is the existence of, or absence of, a connection. This feature of the invention is supported by the above-

referenced passages of Applicants' Specification in enabling one skilled in the art to make and/or use the security aspects of Applicants' claimed invention.

Regarding the Examiner's questions on page 6 of the Office Action: (i) "...it is not clear what is being measured regarding the security characteristic..."; and (ii) "Is the measure of indication of connectivity pertains to available bandwidth, traffic load, or the integrity of the network?" It will be appreciated from Applicants' Specification, as detailed above, that the claimed "indication of connectivity" is directed to the existence of, or absence of, a connection. Thus, in accordance with the claimed invention, the "measure" is the existence (or absence of) the connection itself. The particular attributes of such connection (e.g., bandwidth or traffic load) as raised by the Examiner are irrelevant in terms of the claimed invention and do not serve as proper grounds for rejecting Applicants claims under §112, first paragraph. The relevant aspect with regard to the claimed invention is the existence of, or absence of, a connection as clearly indicated by the pending claims and supported by Applicants' Specification.

For the reasons discussed above, the terms "security characteristic" and "an indication of connectivity" comply with the requirements of §112, first paragraph and Applicants respectfully request reversal of the §112, first paragraph rejections thereof.

2. Rejection of Claims 7, 20 and 23 under 35 USC § 112, first paragraph

The Office Action separately rejected claims 7, 20 and 23 under 35 USC § 112, first paragraph, as failing to comply with the enablement requirement, in particular, with respect to the claimed "different security levels". In so rejecting such claims, the Examiner asserts (see, Office Action, page 6) that "the claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected or with which it is most nearly connected, to make and/or use the invention".

With respect to the claimed "different security levels", such subject matter is supported in at least the following passages of Applicants' Specification: (i) page 8, lines 5-11; (ii) page 10, lines 5-20; (iii) page 6, lines 1-9; and (iv) page 6, lines 10-26. At a minimum, such passages from Applicants' Specification enable one skilled in the art to recognize that the claimed "different security levels" aspect of Applicants' invention is

directed to ascertaining the security of different types of networks, e.g., an intranet vs. the Internet, or a corporate backbone vs. an external network. One skilled in the art will clearly recognize that such disparate networks may have "different security characteristics" which are well-known and typically specified by the network's system administrators. For example, the computer network security characteristics which are addressed by such network administrators include the examples of the types of security threats detailed in Applicants' Specification beginning on page 1, line 25 and continuing at least through page 4, line 16. Such varying security characteristics together with well-known network types (e.g., intranets, Internet, private networks, public networks, etc.) will be readily apparent to those skilled in the art, and in addition to the descriptions of such aspects of the claimed invention in Applicants' Specification, will enable one skilled in the art to make and/or use such claimed invention.

Regarding the Examiner's question on page 6: "Does different security levels means access authentication for users, or security policy implemented on the network in general and on firewall in particular?" It will be appreciated from Applicants' Specification, as detailed above, that the claimed "different security levels" between the first and second networks is directed to the most basic of principles, that is, that the first and second networks have differing (i.e., not the same; dissimilar; distinct; or separate) security levels. For example, as will be readily appreciated by those skilled in the art, a private network and public network will have differing needs with respect to security levels. That is, the degree of the differing security levels (or the specific implementation or delivery of thereof) is not the focus of the claimed invention. Rather, the relevant aspect with regard to the claimed invention, as recited in claims 7, 20, and 23, is that the first and second communications network have different security levels.

For the reasons discussed above, the "different security levels" as claimed by Applicants complies with the requirements of §112, first paragraph and Applicants respectfully request reversal of the §112, first paragraph rejections.

3. Rejection of Claims 1-3, 6-12 14-24 and 26-27 under 35 USC § 102(e)

Claims 1-3, 6-12 14-24 and 26-27 stand rejected under 35 USC § 102(e) as being anticipated by Shostack.

A. Independent Claims 1, 10, 16, 21 and 24

Applicants' claimed invention is directed at ascertaining the integrity of a communications network and thereby identifying potential security risks across the perimeter of such network. An aspect of the invention is directed to the determination of a security characteristic of a host (or hosts) associated with a first communications network wherein the security characteristic is a measure of connectivity between the first communications network and a second communications network. That is, the host (associated with a first network) is probed with a particular packet, where the packet is intentionally configured with a source address which is associated with the second communications network, and the connectivity measure is determined as a function of a response (or lack thereof) from the probed host to the probe packet (see, e.g., Applicants' Specification, page 4, line 27 – page 5, line 6; and page 8, line 23 – page 10, line 28).

Importantly, the source address is selected such that the IP address is external to the probed host's network, that is, the originator address is "false or derived" in that it does not originate from an actual host request (see, e.g., Applicants' Specification, page 9, lines 25-29). Thus, in accordance with the claimed invention, as set forth in the currently pending claims, the source address is selected independent of any actual request (e.g., an information request) from the second host to the first host. Thus, by probing the connectivity of the particular host(s) within a network, in accordance with the claimed invention, an analysis of the network can be made to identify potential security risks across the perimeter of the particular network.

As stated previously, Applicants' an aspect of the claimed invention is directed at discovering connectivity of, or between, a host machine (or host machines) as a function of a response (or absence thereof) to a specifically configured probe packet. In brief, it is the determination of such connectivity measure using the probe packet (configured in accordance with the invention) that is, at a minimum, the contribution advanced by the Applicants over the cited prior art. Applicants have realized that so-called "spoofed

packets" can serve different (i.e., different from that taught by the prior art) purposes (and non-malicious purposes) by providing an enhanced security tool for discovering the connectivity between networks. This connectivity measure, in turn, can be used by system administrators to identify potential security risks across a network's perimeter and prevent malicious attacks.

Each of Applicants' pending independent claims particularly claim the above-described aspects of the invention. For example, pending independent claim 1 recites:

> "A communications network security method for ascertaining the integrity of a first communications network and identifying potential security risks across a perimeter of the first communications network, the method comprising:
>
> identifying a plurality of routes that define the first communications network;
>
> identifying a plurality of hosts associated with the first communications network as a function of the plurality of routes;
>
> receiving a census of the first communications network as a function of the plurality of hosts to determine a topology of the first communications network;
>
> probing at least one first host of the plurality hosts of the first communications network by transmitting a packet to the first host, the first host being selected from the census results and the packet having at least a source address of a second host which is associated with a second communications network, wherein the source address is selected independent of any request from the second host to the first host; and
>
> determining a security characteristic of the probed first host as a function of a response by the probed first host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network." (emphasis added by Applicants)

Each of the currently pending independent claims contains similar limitations, as those set forth in independent claim 1, directed to the above-described features of the invention. As such, contrary to the Examiner's assertion in the Office Action (see, Office Action, page 5), Applicants have particularly pointed out and distinctly claimed the subject matter that Applicants regard as the invention and that which, at a minimum, defines patentable subject matter over the cited prior art.

More particularly, Applicants' understand Shostack to teach a computer security system directed to providing real-time updates which provide updated information related

to so-called "security vulnerabilities" (see, Shostack, column 1, lines 31-43). Further, Shostack's security system provides for a so-called "network security detector" which monitors security intrusions on a network (see, Shostack, column 1, lines 61-65). Shostack's teaching with regard to "IP spoofing" (see, e.g., column 1, line 64 – column 2, line 3; and column 4, lines 52-57) is consistent with known prior art spoofing as discussed hereinabove in the "Summary of Claimed Subject Matter" section.

Shostack's technique tests for susceptibility to the defined security vulnerabilities, such security vulnerability including IP spoofing. For example, Shostack, at column 12, lines 50-55, describes an aspect of Shostack's technique which "...probes the ports of each of the IP devices for programs that contain security vulnerabilities that may be exploited...". Shostack's "security vulnerabilities", as referenced throughout such disclosure, are of the type listed in Shostack's Table 1 (see, e.g., Shostack, columns 5 and 6). While it is true that one such Shostack security vulnerability is a "check of the firewall for IP spoofing" (see, Shostack, column 5, lines 59-60) or "...assess the security vulnerabilities of a remote computer connected to the network..." (see, Shostack, column 13, lines 2-3), these are not disclosures that are fatal to the novelty of Applicants' claimed invention, as detailed further hereinbelow.

In support of the outstanding rejection of Applicants' pending claims, the Office Action relying on Shostack (the "cited prior art") asserts beginning on page 3 that:

> "...The system of cited prior art teaches and describes a computer security system modules for accessing security vulnerabilities on networks such as internet, intranet, extranet, etc. where modules (74,76,78) are used for accessing a data base and the security vulnerability of a computer network, and modules (88,90) are used for accessing security vulnerability of a remote computer connected to the network and for receiving and updating to data base respectively."

The Office Action continues on page 4:

> "Cited prior art teaches a fourth module of this system which allows a remote computer to first connect to a network service and like the second network module, interrogates the service...Therefore module four does this from a remote location. The remote location would then have a source address associated with a second communications network. An address that is different from the first communications network."

Further on page 4 of the Office Action:

> "...Cited prior art also teaches a sixth module which is a communication module that allows an integrated security system to communicate with a similar system over a computer network. In line 27, the module invokes remote systems. In line 34, Shostack teaches that this sixth checks the integrity of the service connection. This teaching is another example of communication between networks to perform the security functions of cited prior art invention."

Applicants respectfully submit that Shostack's fourth module (and, for that matter Shostack's second or sixth module) is not performing, and does not anticipate, teach or suggest, Applicants' claimed invention. In particular, the fact that Shostack's fourth module essentially implements—on a remote basis—the functionality of the second module does not teach or suggest Applicants' claimed invention. That is, remote functionality (an example of which is Shostack's fourth module) does not anticipate Applicants' claimed invention. Shostack, at column 12, lines 41-55, states:

> "The second module 76 accesses the database of security vulnerabilities 92 and assesses network security. The second module 76 connects to a network service, accepts information from the service and interrogates the service. The second module 76 performs a network scan and...The network scan produces a map of the network 86 that is essentially an inventory of the Internet Protocol (IP) devices connected to the network. Using network protocol, the integrated system also probes the ports of each of the IP devices for programs that contain security vulnerabilities that may be exploited.. The network scan ensures that the network 20 and a local server 18 is protected against any unauthorized access that may penetrate the firewall 12." (emphasis added by Applicants)

Shostack's second and fourth modules may be used to determine whether a service engaged by a host computer (including a remote host) is vulnerable to a known set of security vulnerabilities (in particular, Shostack's "security vulnerabilities 92"). Shostack's sixth module teaches a "communications module" which performs well-known system functions such as maintaining communication between Shostack's modules and/or other similar systems, database sharing, report generation/analysis, security and checking the integrity of existing service connections (see, e.g., Shostack, column 13, lines 18-36). As pointed out in the Office Action Shostack's fourth (and second) module require a connection from the remote (or local) computer to "accept

information from the service" (see, e.g., the Shostack column 12 passage hereinabove) and after the establishment of such connection, such modules "interrogate" the network service to determine whether there is a susceptibility to Shostack's identified security vulnerabilities. As such, there is a dependency upon the established connection in the context of Shostack's security vulnerability checking. That is, as set forth in the above Shostack passage, Shostack's second module (and therefore, the fourth which according to Shostack operates similarly but on a remote basis) connects to a network service, accepts information from the service and then interrogates the service. Again, mere remote functionality between one or more networks is not the focus of Applicants' invention and not a teaching that anticipates the claimed invention herein.

In contrast to Shostack, Applicants' claimed invention does not require the establishment of any such connection. Indeed, it the existence and detection of connections between networks (in particular, a rogue connection) that is a focus of Applicants' invention. That is, Applicants' claimed invention is directed to determining whether a connection exists between a host on a first network and as host on a second network utilizing the probe packet configured in accordance the claimed invention, where the source address is selected independent of any request from the second host to the probed host. The probe packet, configured in accordance with the invention, facilitates the delivery of the security aspects of Applicants' invention.

Applicants do not dispute that Shostack's fourth module allows a remote computer to first connect to a network service then accepts information from the service and like the second module also interrogates the services (see, e.g., Shostack, column 13, line 3-6). As mentioned above, Shostack's teaching requires a connection from the remote (or local) computer and after the establishment of such connection, such modules "interrogate" the network service in accordance with Shostack's security vulnerabilities. Applicants do dispute, and disagree with, the suggestion that such teaching anticipates the claimed invention herein.

In particular, none of the cited Shostack modules (i.e., the second, fourth or sixth modules) teach or suggest the principles of the Applicants' claimed invention whereby the specifically configured probe packet is used to determine a connectivity measure between two hosts associated with two communications networks, where the packet

includes a source address which is associated with a second communications network such that the source address is selected independent of any actual request from the second host (of the second network) to the probed host (of the first network). In accordance with the invention, the probe packet is used to identify potential unsecure or rogue connections between a probed host (of a first communications network) and the host on a second communications network. Said another way, Applicants' claimed invention is directed at discovering—as function of the sending/receiving of the claimed probe packet and the response by the probed host to the receipt thereof—connectivity of, or between, a host machine (or host machines).

The Examiner in the Office Action states, on page 5, that the Examiner is "...merely trying to interpret the claim language in its broadest and reasonable meaning...in view of the specification". Of course, it is well settled that "During examination, claims are to be given their broadest reasonable interpretation consistent with the specification, and ...claim language should be read in light of the specification as it would be interpreted by one of ordinary skill in the art." In re American Academy of Science Tech Center, 367 F.3d 1359, 70 U.S.P.Q. 2d 1827, quoting In re Bond, 910 F.2d 831, 833 (Fed.Cir. 1990), 15 U.S.P.Q. 2d 1566.

Further, it is also well settled that "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.". Verdegaal Bros. Inc. v. Union Oil Co., 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987).

However, the breadth of Examiner's interpretation of the pending claim language is so broad (the breadth of which Applicants submit is inconsistent with an interpretation by one of ordinary skill in the art) it leads to an evisceration of the claimed features of the invention as set forth in the currently pending claims. The two Shostack teachings primarily relied on by the Examiner (see, Office Action, pages 4-5) involve remote functionality and a communications module that allows an integrated security system to communication with a similar system over a computer network. From such reliance and the stated breadth of interpretation, the Examiner states (on page 4 of the Office Action) that "The examiner has pointed to two separate teaching where cited prior art teaches or suggests utilizing a probe packet to determine a connectivity measure between two

communications networks where the packet includes a source address which is associated with a second communications network."

As detailed above, Applicants' claimed invention requires that a host (associated with a first network) is probed with a particularly configured packet, where the packet is intentionally configured to include a source address which is associated with a second host on the second communications network but independent of any actual request from the second host to the probed host. Thereafter, in accordance with the invention, the connectivity measure is determined as a function of a response (or lack thereof) from the probed host to the receipt of the probe packet. The Examiner has not pointed to any specific probe packet and use thereof, as claimed by Applicants, that is taught or suggested by Shostack.

Further, the Examiner's stated "broadest interpretation" attempts to read the claim language in such a way to distort the claimed invention. That is, as discussed above, Shostack's fourth (and second) module require a connection from the remote (or local) computer and after the establishment of such connection, such modules "interrogate" the network service in accordance with Shostack's security vulnerabilities. No such pre-existing connection is required or claimed by Applicants' invention. Indeed, it is the prior existence of, or lack thereof, a such a connection to which an aspect of Applicants' claimed invention is directed in determining a connectivity measure between two communication networks which can be used to identify potential unsecure or rogue connections between the probed host (of a first communications network) and some other host on the second communications network, as detailed above.

Therefore, the Office Action has failed to establish a *prima facie* case of anticipation, at a minimum, in that Shostack does not disclose such aspects of Applicants' claimed invention directed to the determination of a security characteristic of a host (or hosts) associated with a first communications network wherein the security characteristic is a measure of connectivity between the first communications network and a second communications network, whereby the host (associated with a first network) is probed with a particular packet, where the packet is intentionally configured to include a source address which is associated with a second host on the second communications network but independent of any actual request from the second host to the probed host, and the

connectivity measure is determined as a function of a response (or lack thereof) from the probed host to the receipt of the probe packet.

B. Dependent Claims

Regarding the rejection of each of the presently pending dependent claims under 35 USC § 102(e), these claims depend ultimately from one of the pending independent claims 1, 10, 16, 21 and 24 herein which Applicants submit are patentably distinct over Shostack for the aforesaid reasons. Thus, these dependent claims contain all the limitations of the pending independent claims from which they depend, and Applicants respectfully submit that these dependent claims are also patentably distinct over Shostack for the aforesaid reasons, as well as other elements these claims add in combination to their base claim.

4. Rejection of Claim 14 under 35 USC § 103(a)

The Office Action rejected claim 14 under 35 USC § 103(a) as being unpatentable over Shostack in view of Sitaraman et al.

In order to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference, or combination of references, must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based an applicant's disclosure (see, MPEP § 2142 citing In re Vaeck, 947 F.2d 488, 20 U.S.P.Q. 2d. 1438 (Fed. Cir. 1991)). Applicants respectfully submit that the Office Action fails to establish a *prima facie* case of obviousness. More particularly, Applicants respectfully submit that combining the teaching of Sitaraman with that of Shostack would provide Shostack's security system with the further feature of forced sequential access thereby forcing authorized users in Shostack's system to disconnect from any open connections to other public or private

domains or networks before a connection with the user's domain can be established (see, e.g., Sitaraman, column 4, lines 36-41).

Even assuming *arguendo* that such a combination is proper and one skilled in the art would be motivated to so combine such teachings, nothing in the Shostack/Sitaraman combination teaches or suggests utilizing the probe packet of the present invention to determine a connectivity measure between two communication networks which can be used to identify potential unsecure or rogue connections between a probed host (of a first communications network) and some other host on a second communications network, as detailed above. Further, nothing in the Shostack/Sitaraman combination teaches or suggests the aspects of Applicants' claimed invention, as set forth in pending claim 14, which is directed to the determination of a security characteristic of a host (wherein such host is a dual-homed host as set forth in pending claim 14; see also, Applicants' Specification, page 8, lines 3-11) associated with a first communications network wherein the security characteristic is a measure of connectivity between the first communications network and a second communications network, whereby the dual-homed host is probed with a particular packet, where the packet is intentionally configured to include a source address which is associated with a second host on the second communications network but independent of any actual request from the second host to the probed dual-homed host, and the connectivity measure is determined as a function of a response (or lack thereof) from the probed dual-home host to the receipt of the probe packet.

5. Conclusion

In view of the foregoing, Applicants hereby request that the rejections of claims 1-3, 6-12, 14-24 and 26-27 be reversed and the application promptly allowed. The attention of the Examiner and the Appeal Board in this matter is appreciated.

Respectfully submitted,

Steven Branigan
Hal Joseph Burch
William R. Cheswick

By _____
Donald P. Dinella
Attorney for
Applicants/Appellants
Reg. No. 39,961
908-582-8582

Date: December 6 2005

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030

CLAIMS APPENDIX

Claims Involved in this Appeal

1. A communications network security method for ascertaining the integrity of a first communications network and identifying potential security risks across a perimeter of the first communications network, the method comprising:

identifying a plurality of routes that define the first communications network;

identifying a plurality of hosts associated with the first communications network as a function of the plurality of routes;

receiving a census of the first communications network as a function of the plurality of hosts to determine a topology of the first communications network;

probing at least one first host of the plurality hosts of the first communications network by transmitting a packet to the first host, the first host being selected from the census results and the packet having at least a source address of a second host which is associated with a second communications network, wherein the source address is selected independent of any request from the second host to the first host; and

determining a security characteristic of the probed first host as a function of a response by the probed first host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network.

2. The method of claim 1 wherein the source address of the second host is a return IP address external to the first communications network.

3. The method of claim 2 wherein the response of the probed first host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet.

4. (Cancelled).

5. (Cancelled).

6. The method of claim 2 wherein the measure of connectivity is determined by the further operation of:

monitoring the probed first host to determine the response, and if the response includes a transmission of a second packet from the probed first host to the second host at the return IP address, generating a security alert message identifying the probed first host as a security risk.

7. The method of claim 3 wherein the first communications network and the second communications network have different security levels.

8. The method of claim 3 wherein the transmitted packet is a TCP packet which returns a TCP packet in response thereto.

9. The method of claim 3 wherein the second packet is a UDP packet or an ICMP packet, which returns either a UDP packet or ICMP packet in response thereto.

10. A method for analyzing network security across a perimeter of a first communications network utilizing a security host, the method comprising:

receiving a census of the first communications network;

transmitting, from the security host, a packet associated with a host of a second communications network to a particular one host of a plurality of hosts internal to the first communications network, the internal host being selected from the census, and the packet having an IP source address associated with the host of the second communications network, wherein the IP source address is selected independent of any request from the host of the second communications network to the internal host of the first communications network; and

determining a security characteristic of the particular one internal host of the first communications network as a function of a response by the internal host to the receipt of the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network, the measure of

connectivity being an indication of connectivity between the first communications network and the second communications network.

11. The method of claim 10 wherein the measure of connectivity is a function of whether the internal host of the first communications network communicates with the host of the second communications network, and the measure of connectivity being determined by the further operation of:

monitoring the internal host to determine the response, and if the response includes a transmission of a second packet, utilizing the IP source address, from the internal host to the host of the second communications network, generating a security alert message identifying the internal host as a security risk.

12. The method of claim 11 wherein the second packet is derived using at least a portion of information from the transmitted packet.

13. (Cancelled).

14. The method of claim 12 wherein the internal host is a dual-homed host.

15. The method of claim 11 wherein the security characteristic includes an indication that the internal host is outside any security measures provided by a firewall associated with the first communications network.

16. A communications system for ascertaining the integrity of a first communications network and identifying potential security risks across a perimeter of the first communications network, the communications system comprising:

a first plurality of computers associated with the first communications network;

a second plurality of computers associated with a second communications network; and

a security host computer which determines a security characteristic of a first computer from the first plurality of computers, the security characteristic being a measure

of connectivity between the first communications network and the second communications network by probing the first computer by transmitting a packet to the first computer, the first computer being selected from a census of the first communications network and the packet being generated as a function of both an IP source address associated with a second computer of the second plurality of computers, wherein said IP source address is selected independent of any request from the second computer to the first computer, and an IP address associated with the first computer, and determining the measure of connectivity as a function of a response of the first computer to receiving the packet, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network.

17. The communications system of claim 16 wherein the security host computer is associated with the first communications network.

18. The communications system of claim 17 wherein the response of the first computer to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet.

19. The communications system of claim 18 wherein the security host computer determines the measure of connectivity by monitoring the probed first computer to determine the response, and if the response includes the transmission of the second packet from the probed host, generating a security alert message identifying the first computer as a security risk.

20. The communications system of claim 17 wherein the first communications network is an intranet and the second communications network is an Internet, and the first communications network and the second communications network have different security levels.

21. A security host computer for ascertaining the integrity of a first communications network and identifying potential security risks across a perimeter of the first communications network, the security host computer comprising:

means for performing a census of the first communications network and determining a topology of the first communications network, the topology being defined by at least one computer,

means for probing the at least one computer by transmitting a packet to the computer, the computer being selected from the census results and the packet being generated as a function of (i) the topology, (ii) an IP source address associated with a particular host computer associated with a second communications network, wherein the IP source address is selected independent of any request from the second computer to the first computer, and (iii) an IP address associated with the computer, the second communications network being separate from the first communications network; and

a monitor for determining a security level of the computer as a function of a response by the computer to the receipt of the packet, and the security level being a measure of connectivity between the first communications network and the second communications network, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network.

22. The security host computer of claim 21 wherein the measure of connectivity is determined by monitoring the computer's response, and if the response includes a transmission of a second packet, utilizing the IP source address, from the computer, a security alert message identifying the computer as a security risk is generated.

23. The security host computer of claim 22 wherein the first communications network and the second communications network have different security levels.

24. A machine-readable medium having stored thereon a plurality of instructions, the plurality of instructions including instructions that, when executed by a machine, cause the machine to perform of a method for analyzing a first communications network's integrity and identifying potential security risks across a perimeter of the first

communications network by receiving a census of the first communications network; probing a first host of the first communications network by transmitting a packet to the first host, the host being selected from the census results and the packet being derived as a function of a topology of the first communications network and the packet having a source address which is associated with a second host of a second communications network, wherein the source address is selected independent of any request from the second host to the first host; and determining the first communications network's integrity as a function of a response by the probed host in receiving the packet wherein the response indicates a measure of connectivity between the first communications network communicates and the second communications network, and the measure of connectivity being an indication of connectivity between the first communications network and the second communications network.

25. (Cancelled).

26. The machine-readable medium of claim 24 wherein the response of the probed first host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet.

27. The machine-readable medium of claim 26 wherein the first communications network is an intranet, and the second communications network is an Internet.

EVIDENCE APPENDIX

Enclosures:
Copy of TechTV (www.techtv.com) excerpt
Copy of Computerworld (www.computerworld.com) excerpt

The above-referenced enclosures were also set forth in an Amendment, dated April 7, 2004, submitted by Applicants/Appellants in the subject application.

Are you afraid of one company owning all your local news?

- ○ Yes, the FCC frightens me
- ○ A little, I use the Internet for news
- ○ No, one company still can't own all my town's media
- ○ Hey, just don't take away my 'Temptation Island 7'!

Bill Cheswick's bag of tricks
Firewall and Internet security expert Cheswick tells us what's in his bag of tricks.

Sarah's shopping tip: Additional buys
Sure, $30 for a new printer is enticing, but make sure you know what you're getting. Many printers don't include the cables you need to connect to your computer. Some don't even include consumables such as ink and paper. Make sure you consider these items in your budget.

Join our LAN Party
Frag fellow fans (and staff members) in the only live, televised LAN party in the world. Our LAN Party is held every Thursday, but you must register to participate.

Digital video tips
Tips to make your digital videos look professional.

Tonight on 'Tech Live'
Not all actors are Vin Diesel and can perform high-risk action shots. That's where stuntmen and stuntwomen come in. This weekend, they're being honored at the annual World Stunt Awards. "Tech Live" is there and has all the action.

Real Deal
There are lots of good deals, lots of not-so-good deals, and lots of deals where you should read the fine print before making a purchase.

- **Deal No. 1: PDAs**
  - **Product:** Palm and Pocket PC PDAs
  - **Advertisers:** Various retailers
  - **Patrick and Jessica's comments:** Father's Day is around the corner, so you might be thinking that a PDA would make a great present. Think twice. Be honest about what your father really needs and uses. If your father isn't an organizer-type guy, or if he's averse to using such practical technology, the PDA will end up being an expensive paperweight.
- **Deal No. 2: PVRs**
  - **Product:** TiVo
  - **Advertisers:** Various retailers
  - **Patrick and Jessica's comments:** While a PDA may not

Lessons learned from the Blaster worm

Advice by Peter H. Gregory

SEPTEMBER 24, 2003 (COMPUTERWORLD) - Blaster, Nachi and their variants were worms that attacked a Windows security flaw found on most end-user workstations. Companies that were hit with these worms discovered weaknesses in their architectures, processes and procedures that weren't considered important until now. I asked some of my colleagues in information security for their comments and lessons learned. They are summarized here.

How the worm got in

Worms penetrated organizations in several ways. A systems administrator in a branch of the U.S. military described how an employee accessed a personal Web mail account from work, downloaded an infected message and opened the attachment, thereby beginning the spread inside the organization. That user's antivirus software had to have been disabled, or it had an out-of-date signature file.

A systems analyst at a parts-distribution company told me that contractors brought in their laptops and routinely connected them to the corporate network without IT's involvement. Some of those laptops had out-of-date signature files or expired antivirus subscriptions, enabling them to become infected while connected to an unprotected home LAN or hot spot.

A help desk employee at a telecommunications company told of laptops that employees took home and connected to their Digital Subscriber Line or cable-modem Internet connections. Their home LANs and laptops were unprotected by firewalls and were scanned and infected, and upon returning to the corporate network, these systems began the spread internally.

Another scenario involved network connections between companies. The parts-distribution company mentioned earlier used router-based virtual private network (VPN) technology to encrypt network traffic between companies. The company on the far end of the VPN link was hit pretty hard with Blaster, filling the VPN connection with Blaster scanning traffic that was then able to begin infecting systems on the near side of the VPN connection. The trouble in this case was that the VPN connection, while encrypted, didn't have a firewall. The company permitted all network traffic from the other company to pass unhindered, including Blaster worm scanning traffic.

In all of these cases, antivirus software wasn't working, was expired or wasn't updating virus signature files often enough, or at all.

How the worm spread

Once an infected system began scanning for more systems, any systems lacking the security patch and up-to-date antivirus signatures also became infected.

No organizations I talked with had any internal firewalls. As well-known Internet security expert Bill Cheswick used to say, these organizations had networks with soft, chewy centers. Once a worm was inside the organization, there were no internal firewalls to stop its spread. If you have trouble picturing this, then think about why navy ships and submarines have several watertight compartments sealed with bulkheads. A breach in one compartment won't threaten to sink the ship.

Peter H. Gregory, CISSP, CISA, is an information technology and security consultant, a freelance writer and an author of several books, including *Solaris Security*, *Enterprise Information Security*, and *CISSP for Dummies*. As a consultant he provides strategic technology and security services to small and large businesses.

He can be reached at p.gregory@hartgregorygroup.com. His Web site is www.hartgregorygroup.com.

Lessons learned

- **Organizations need better control over computers they don't own** and other devices being connected to their internal networks. This can be achieved through policy, awareness and enforcement. For example, Dynamic Host Configuration Protocol (DHCP) servers should be made smarter about allocating IP addresses only to systems they recognize and not just any device on the network capable of generating a DHCP request.

- **Organizations are learning that the network perimeter exists in many places besides the Internet firewall.** Connections to other organizations, and even connections within organizations, also need to have firewalls. Company laptops need to take a little piece of the perimeter with them when they travel outside the corporate firewall. Organizations need to consider installing personal firewall software on laptops to protect them from external threats when they're connected to the Internet via an unfirewalled home network or hot spot.

- **Antivirus software is only as good as its signature files are up-to-date.** This can be challenging in large, distributed organizations. Nevertheless, more care over antivirus software and the mechanisms used to update signature files may be in order for many organizations.

- **Companies that had scaled back their PC support departments were hit hard** because they didn't have enough resources to disinfect systems quickly. As a result, some companies spent several days trying to keep up with cleaning infected systems and taking calls from users complaining of slow networks. Companies that had outsourced PC support to off-site organizations also felt the pain, since there were no on-site PC technicians to install patches when they needed to be physically present to do so.

While most of these lessons have been best practices for years, I hope organizations that were hit with Blaster or Nachi put these lessons into practice before the next Internet worm makes the rounds.

Blaster Worm - Recent Headlines

> Security highlights from around the Web

> Sidebar: Antivirus Software Vendors Fuel Mydoom Hype

> Dual curses: Viruses and spam

> New Tools Shift Focus to Internal Network Security

View our Blaster Worm special coverage page

Coverage of the Blaster worm and its aftermath.

RELATED PROCEEDINGS APPENDIX

None.